

CLAIMS

1. Apparatus for requesting authentication comprising:
 - a storage medium configured to store a cryptographic key;
 - a processor coupled to the storage medium and configured to generate an access code using the cryptographic key;
 - a converter coupled to the processor and configured to convert the access code into sound waves encoded with the access code; and
 - an audio output unit coupled to the converter and configured to output the sound waves encoded with the access code for authentication.
2. The apparatus of claim 1, wherein the cryptographic key is a private key corresponding to a public key.
3. The apparatus of claim 1, wherein the cryptographic key is a symmetric key.
4. The apparatus of claim 1, further comprising:
 - a clock coupled to the processor and configured to generate a time element;and wherein
 - the processor is configured to generate the access code using the cryptographic key and the time element.
5. The apparatus of claim 1, further comprising:
 - an audio input unit configured to receive sound waves encoded with a challenge; wherein
 - the converter recovers the challenge; and
 - the processor is configured to generate the access code using the cryptographic key and the challenge.
6. The apparatus of claim 5, wherein the audio input unit comprises a microphone.
7. The apparatus of claim 1, wherein the audio output unit comprises a speaker.

8. The apparatus of claim 1, further comprising:
an actuator coupled to the processor and configured to receive a signal that activates the generation of the access code.
9. The apparatus of claim 1, further comprising:
a user input unit configured to receive a first password; wherein
the storage medium is configured to store a second password; and wherein
the processor is configured to generate the access code if the first password corresponds to the second password.
10. The apparatus of claim 1, further comprising:
a user input unit configured to receive a password; wherein
the converter is configured to encode the password into sound waves; and
wherein
the audio output unit is configured to output the sound waves encoded with the password for authentication.
11. A method for requesting authentication from a user device storing a cryptographic key, comprising:
generating an access code using the cryptographic key;
converting the access code into sound waves encoded with the access code;
and
outputting the sound waves encoded with the access code for authentication.
12. The method of claim 11, wherein the cryptographic key is a private key corresponding to a public key.
13. The method of claim 11, wherein the cryptographic key is a symmetric key.
14. The method of claim 11, further comprising:
generating a time element; wherein
generating the access code comprises generating the access code using the cryptographic key and the time element.

15. The method of claim 11, further comprising:
receiving sound waves encoded with a challenge; and
recovering the challenge; wherein
generating the access code comprises generating the access code using the cryptographic key and the challenge.
16. The method of claim 11, further comprising:
receiving a signal that activates the generation of the access code.
17. The method of claim 11, wherein the user device stores a first password and the method further comprises:
receiving a second password; wherein
generating the access code comprises generating the access code if the first password corresponds to the second password.
18. The method of claim 11, further comprising:
receiving a password;
encoding the password into sound waves; and
outputting the sound waves encoded with the password for authentication.
19. Apparatus for requesting authentication comprising:
means for storing a cryptographic key;
means for generating an access code using the cryptographic key;
means for converting the access code into sound waves; and
means for outputting the sound waves encoded with the access code for authentication.
20. The apparatus of claim 19, wherein the cryptographic key is a private key corresponding to a public key.
21. The apparatus of claim 19, wherein the cryptographic key is a symmetric key.
22. The apparatus of claim 19, further comprising:
means for generating a time element; wherein

the means for generating the access code generates the access code using the cryptographic key and the time element.

23. The apparatus of claim 19, further comprising:
means for receiving sound waves encoded with a challenge; and
means for recovering the challenge; wherein
the means for generating the access code generates the access code using the cryptographic key and the challenge.
24. The apparatus of claim 19, further comprising:
means for receiving a signal that activates the generation of the access code.
25. The apparatus of claim 19, further comprising:
means for receiving a first password; and
means for storing a second password; wherein
the means for generating the access code generates the access code if the first password corresponds to the second password.
26. The apparatus of claim 19, further comprising:
means for receiving a password;
means for encoding the password into sound waves; and
means for outputting the sound waves encoded with the password for authentication.
27. A machine readable medium for use in requesting authentication comprising:
code segment configured to generate an access code using a cryptographic key;
code segment configured to convert the access code into sound waves encoded with the access code; and
code segment configured to output the sound waves encoded with the access code for authentication.
28. The medium of claim 27, further comprising:
code segment configured to generate a time element; wherein

the code segment for generating the access code generates the access code using the cryptographic key and the time element.

29. The medium of claim 27, further comprising:
code segment configured to receive sound waves encoded with a challenge;
and
code segment configured to recover the challenge; wherein
the code segment for generating the access code generates the access code using the cryptographic key and the challenge.
30. Apparatus for authenticating comprising:
a storage medium configured to store a cryptographic key;
an audio input unit configured to receive sound waves encoded with an access code;
a converter coupled to the audio input unit and configured to recover the access code from the sound waves; and
a processor coupled to the storage medium and the converter, the processor configured to verify the access code based on the cryptographic key and to grant access if the access code is verified.
31. The apparatus of claim 30, wherein the cryptographic key is a public key corresponding to a private key.
32. The apparatus of claim 30, wherein the cryptographic key is a symmetric key.
33. The apparatus of claim 30, further comprising:
a clock coupled to the processor and configured to generate a time element;
wherein
the processor is configured verify the access code using the cryptographic key and the time element.
34. The apparatus of claim 30, further comprising:
an audio output unit configured to output sound waves encoded with a challenge; wherein

the processor is configured to generate the challenge; and
the converter is configured to encode the challenge into the sound waves encoded with the challenge;
the processor is configured to verify the access code using the cryptographic key and the challenge.

35. The apparatus of claim 34, wherein the audio output unit comprises a speaker.

36. The apparatus of claim 34, wherein
the storage medium is configured to store a first password;
the audio input unit is configured to receive sound waves encoded with a second password;
the converter is configured to recover the second password; and
the processor is configured to generate the challenge if the first password corresponds to the second password.

37. The apparatus of claim 34, further comprising:
receiver unit configured to receive a first password; wherein
the storage medium is configured to store a second password; and
the processor is configured to generate the challenge if the first password corresponds to the second password.

38. The apparatus of claim 30, wherein the audio input unit comprises a microphone.

39. The apparatus of claim 30, wherein
the storage medium is configured to store a first password;
the audio input unit is configured to receive sound waves encoded with a second password;
the converter is configured to recover the second password; and
the processor is configured to verify the access code if the first password corresponds to the second password.

40. The apparatus of claim 30, further comprising:

receiver unit configured to receive a first password; wherein
the storage medium is configured to store a second password; and
the processor is configured to verify the access code if the first password
corresponds to the second password.

41. A method for authenticating in a verifier device storing a cryptographic key,
comprising:

receiving sound waves encoded with an access code;
recovering the access code from the sound waves encoded with an access
code; and
verifying the access code based on the cryptographic key.

42. The method of claim 41, wherein the cryptographic key is a public key
corresponding to a private key.

43. The method of claim 41, wherein storing the cryptographic key is a symmetric
key.

44. The method of claim 41, further comprising:
generating a time element; wherein
verifying the access code comprises verifying the access code based on the
cryptographic key and the time element.

45. The method of claim 41, further comprising:
generating a challenge;
encoding the challenge into the sound waves encoded with the challenge;
outputting sound waves encoded with a challenge; wherein
verifying the access code comprises verifying the access code based on the
cryptographic key and the challenge.

46. The method of claim 45, wherein the verifier device stores a first password
and the method further comprises:

receive sound waves encoded with a second password; and
recovering the second password; wherein

generating the challenge comprises generating the challenge if the first password corresponds to the second password.

47. The method of claim 45, wherein the verifier device stores a first password and the method further comprises:

- receiving a second password; wherein
- generating the challenge comprises generating the challenge if the first password corresponds to the second password.

48. The method of claim 41, wherein the verifier device stores a first password and the method further comprises:

- receiving sound waves encoded with a second password; and
- recovering the second password; wherein
- verifying the access code comprises verifying the access code if the first password corresponds to the second password.

49. The method of claim 41, wherein the verifier device stores a first password and the method further comprises:

- receiving a second password; wherein
- verifying the access code comprises verifying the access code if the first password corresponds to the second password.

50. Apparatus for authenticating comprising:

- means for storing a cryptographic key;
- means for receiving sound waves encoded with an access code;
- means for recovering the access code from the sound waves; and
- means for verifying the access code based on the cryptographic key.

51. The apparatus of claim 50, wherein the means for storing the cryptographic key stores a public key corresponding to a private key.

52. The apparatus of claim 50, wherein the means for storing the cryptographic key stores a symmetric key.

53. The apparatus of claim , further comprising:
means for generating a time element; wherein
the means for verifying the access code verifies the access code using the
cryptographic key and the time element.
54. The apparatus of claim 50, further comprising:
means for generating a challenge;
means for converting the challenge into the sound waves encoded with the
challenge; and
means for outputting sound waves encoded with a challenge; wherein
the means for verifying the access code verifies the access code based on the
cryptographic key and the challenge.
55. The apparatus of claim 54, further comprising:
means for storing a first password;
means for receive sound waves encoded with a second password; and
means for recovering the second password; wherein
the means for generating the challenge generates the challenge if the first
password corresponds to the second password.
56. The apparatus of claim 54, further comprising:
means for receiving a first password; and
means for storing a second password; wherein
the means for generating the challenge generates the challenge if the first
password corresponds to the second password.
57. The apparatus of claim 50, further comprising
means for storing a first password;
means for receiving sound waves encoded with a second password; and
means for recovering the second password; wherein
the means for verifying the access code verifies the access code if the first
password corresponds to the second password.
58. The apparatus of claim 50, further comprising:

means for receiving a first password; and
means for storing a second password; wherein
the means for verifying the access code verifies the access code if the first
password corresponds to the second password.

59. A machine readable medium used for authenticating comprising:
code segment for receiving sound waves encoded with an access code;
code segment for recovering the access code from the sound waves encoded
with the access code; and
code segment for verifying the access code based on the cryptographic key.
60. The medium of claim 59, further comprising:
code segment for generating a time element; and wherein
code segment for verifying the access code verifies the access code based on
the cryptographic key and the time element.
61. The apparatus of claim 59, further comprising:
code segment for generating challenge;
code segment for converting the challenge into audio wave encoded with the
challenge;
code segment for outputting sound waves encoded with a challenge; wherein
the code segment for verifying the access code verifies the access code based
on the cryptographic key and the challenge.